What is claimed is:

1. A network security architecture for monitoring security activities in a mobile network platform, comprising

a mobile network residing on the mobile network platform, the mobile network being interconnected via an unreliable communication link to a terrestrial-based network security management system;

an intrusion detection system connected to the mobile network and residing on the mobile network platform, the intrusion detection system operable to detect a security intrusion event that is associated with the mobile network; and

a mobile security manager residing on the mobile network platform and adapted to receive the security intrusion events from the intrusion detection system, the mobile security manager is further operable to perform security response activities in response to the security intrusion events, when the mobile network platform is not connected with network security management system.

2. The network security architecture of Claim 1 wherein the mobile security manager is operable perform security response activities in accordance with a security policy resident on the mobile network platform.

3. The network security architecture of Claim 2 wherein the security policy is defined as a plurality of predefined security intrusion events and a corresponding security response for each of said plurality of security intrusion events.

4. The network security architecture of Claim 2 wherein the security policy is defined by a data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element, and a security response element.

5. The network security architecture of Claim 1 wherein the mobile network includes a plurality of user access points, such that the security intrusion event is associated with one of the plurality of user access points and the security response is directed to said one of the plurality of user access points.

6. The network security architecture of Claim 5 wherein the security response is selected from the group consisting of logging the security intrusion event received from the intrusion detection system, providing a warning message to at least one of said user access points, providing an alert message to a terrestrial-based network security management system, installing a network traffic blocking filter at one of said user access points, and disconnecting one of said user access points from the mobile network.

7. The network security architecture of Claim 5 wherein the mobile security manager maintains an indicator of the current operational state for each of the plurality of user access points, such that the security response directed to said one of the plurality of user access points is in part based on the operational state of said one of the plurality of user access points.

8. The network security architecture of Claim 7 wherein the current operational state for any given user access point is selected from the group consisting of a normal state, a suspected state, and a disconnect state.

9. The network security architecture of Claim 7 wherein the mobile security manager is further operable to identify the current operational state for said one of the plurality of user access points and perform security response activities based in part on the identified operational state and the security intrusion event received from the intrusion detection system.

10. The network security architecture of Claim 9 wherein the mobile security manager is further operable to modify the current operational state for said one of the plurality of user access points in accordance with the security policy.

11. The network security architecture of Claim 1 wherein the mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the network security management system.

12. A method for monitoring security activities associated with a network residing in a mobile network platform, the mobile network platform being interconnected via an unreliable communication link to a terrestrial-based network security management system, comprising:

detecting a security intrusion event whose origination is associated with the network residing on the mobile network platform;

providing a mobile security manager residing on the mobile network platform, where the mobile security manager is adapted to receive the security intrusion event; and

performing a security response activity in response to the detected security intrusion event, when the mobile network platform is not connected with the network security management system.

13. The method of Claim 12 wherein the step of performing a security response activity further comprises applying the security response activity in accordance with a security policy, where the security policy is defined as a plurality of predefined security intrusion events and a corresponding security response for each of said plurality of security intrusion events.

14. The method of Claim 12 further comprising the steps of applying the security response activity in accordance with a security policy, where the security policy is defined by a data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element, and a security response element.

15. The method of Claim 12 wherein the network includes a plurality of user access points, such that the security intrusion event is associated with one of the plurality of user access points and the security response is directed to said one of the plurality of user access points.

16. The method of Claim 15 wherein the security response activity is selected from the group consisting of logging the security intrusion event, providing a warning message to at least one of the user access points, providing an alert message to a terrestrial-based network security management system, installing a network traffic blocking filter at one of the user access points, and disconnecting one of the user access points from the network.

17. The method of Claim 15 further comprising the steps of maintaining an indicator of the current operational state for each of the plurality of user access points and performing a security response activity in response to the detected security intrusion event, where the security response activity is in part based on the operational state of said one of the plurality of user access points.

18. The method of Claim 17 wherein the current operational state for any given user access point is selected from the group consisting of a normal state, a suspected state, and a disconnect state.

19. An airborne security system for monitoring security activities associated with a network residing on an aircraft, the aircraft being interconnected via an unreliable communication link to a terrestrial-based network security management system, comprising:

an intrusion detection system connected to the network and operable to detect a security intrusion event that is associated with network; and

an airborne security manager connected to the network and adapted to receive the security intrusion event from the intrusion detection system, the security manager is further operable to perform security response activities in accordance with a security policy, when the aircraft is not connected with the network security management system.

D0E0E0E